SECURE COMMUNICATION PROCEDURE FOR ISDN

G J Claassen and G J Kühn

Potelin, Dept of Posts and Telecommunications,
Private Bag X74, Pretoria, 0001.

Dept of Electronic and Computer Eng., University
of Pretoria, Pretoria, 0001.

ABSTRACT

This paper outlines the security requirements of communication networks. An overview of the basic concepts of encryption is given and the key distribution problem which arises when encryption is implemented as the basis of security services in communication networks is analysed. A secure communications procedure based on a hybrid encryption system and an adapted version of the proposed strong three way authentication method of the CCITT and ISO is then described. The paper concludes with a description of the integration of the secure communication procedure in ISDN to perform key distribution in association with a circuit-switched connection.

1.0 INTRODUCTION

Computers and telecommunication systems are increasingly being used to process and transport information that is sensitive to an individual, a company, or society. There are several trends, which the widespread adoption of standard high-level network protocols will intensify, that emphasize the need to develop network security mechanisms.

The security problem can be subdivided into the problem of privacy and the authentication problem. The privacy problem consists in preventing someone other than the legitimate receiver from extracting information from the communication channel; the authentication problem consists in preventing someone other than the legitimate sender from modifying or injecting data into the channel, so that the receiver can be sure that he actually received the original message from the legitimate sender.

The most appropriate and practical means to provide privacy and authentication in communication networks is by using encryption. This paper takes a look at the implementation of encryption in large communication networks and spesifically ISDN. In our present age of standardisation of encryption algorithms, the only element that is still secret is the encryption keys. For this reason special attention will be given to the problems and the implementation of key distribution in ISDN. The following main topics will be covered:

- Overview of basic encryption concepts
- The key distribution problem
- Key distribution fundamentals
- Secure communication procedure for large networks
- Implementation in ISDN

2.0 OVERVIEW OF BASIC ,ENCRYPTION CONCEPTS

Cryptography is too broad a subject to be discussed here in any depth. We will limit ourselves to explain only those concepts necessary for the discussion of a secure communications procedure for ISDN. If more information are required, substantial literature can be found in books and journals [1, 8].

A cipher is an algorithmic transformation performed on a symbol-by-symbol basis on any data. The terms encipherment and encryption refer synonymously to the application of a cipher to data. An encryption algorithm is any algorithm that implements a cipher. The readable input to an encryption algorithm is referred to as a cleartext or plaintext, while the scrambled output from the algorithm is called ciphertext. The transformation performed on the cleartext to encipher it is controlled by a key. For use in the communication context, the encryption algorithm must be invertible; that is, there must be a matching decryption algorithm that reverses the encryption transformation when presented with the appropriate key.

2.1 Encryption systems

Encryption systems can be divided into two classes, i.e. symmetrical (conventional) systems and asymmetrical (public key) systems.

2.1.1 Conventional systems

In conventional systems the encryption and decryption keys are identical. Such a key must be kept secret, known only to authorized users. Authorized users can use the key both to encrypt their own messages, and to decrypt messages that others have encrypted using it. Fig. 1 illustrates these aspects of a conventional system. Keys need to be exchanged between users, often over a slow secure channel, for example a private courier, and the number of keys can be very large, if every pair of users requires a different key. This creates a key distribution

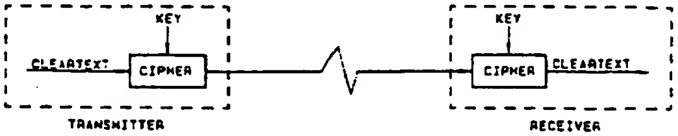


FIGURE 1: A CONVENTIONAL CIPHER

TH0219-6/88/0000-0165 $1.00 © 1988 IEEE

problem which is partially solved in the public key systems. Examples of conventional systems are the Data encryption standard (DES) and rotor ciphers.

2.1.2 Public key systems

In a public-key cipher, the ability to encipher messages under a given key is separated from the ability to decipher those messages. This is accomplished by using pairs of keys. These keys define a pair of transformations, each of which is the inverse of the other, and neither of which is derivable from the other. Each user posesses such a key pair. For user A, one key Ap is made public, for use in encrypting messages for that user while the corresponding key As is kept secret, for use in deciphering messages sent to the user under the public key.

This procedure takes care of the privacy problem, but since anyone can transmit a message to a user A under that user's public key Ap , some additional mechanism is needed to securely identify or authenticate the sender. Identification is accomplished by having the sender B encrypt the message under his secret key Bs , then under the public key of the intended receiver Ap . The receiver can then strip off the outer layer of encryption using his secret key As, and complete the deciphering using the public key of the sender Bp. Anyone with access to the public key can verify that it must have been encrypted with the corresponding secret key, but is of no help in creating (forging) a message. This phenomenon is called a digital signature and is shown in Figure 2.

One of the supposed advantages of a public-key cryptosystem is that public keys may be freely distributed without concern for secrecy. But the need for authentication in the distribution of public keys in an open-system environment results in there being few differences between public-key and conventional-key distribution mechanisms [1].

The most successful implementation of a public key system is the RSA-system [3]. This system makes joint use of the fact that factoring is much harder than multiplying, and that taking either roots or logarithms is much harder than exponentiating. It has recently been proposed by the CCITT and ISO as a strong authentication mechanism for use as part of a directory server [4].

The biggest problem regarding public-key systems is that that they are computationally very involved. Software employing this type of encryption is very slow. The fastest hardware implementation of the RSA achieves bit rates of about 10 kBit/s which is too slow for on line encryption of 64 kBit/s data.

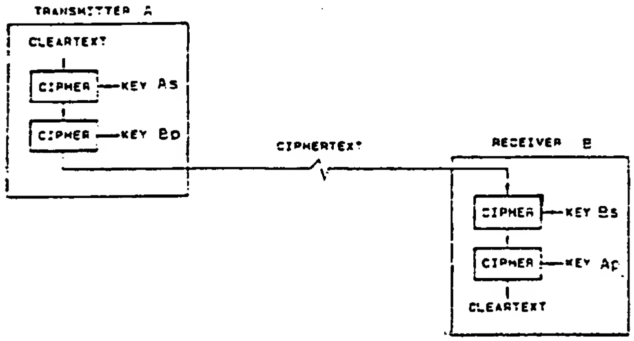


FIGURE 2: A PUBLIC KEY CIPHER

2.2 Approaches to communication security

There are two basic approaches to communication security: link-oriented measures and end-to-end security measures. The former provides security by protecting message traffic independantly on each communication link, while the latter provides uniform protection for each message all the way from its source to its destination. In an open-systems environment end-to-end encryption is generally regarded as superior to link encryption.

3.0 THE KEY DISTRIBUTION PROBLEM

Conventional encryption requires that for ensuring secure communications, communicators must have keys that are identical. This lead to the so called key distribution problem in a large network of communicators who wish to communicate with each other securely. If all communicators in the network are using the same key, and if the key is compromised by any one communicator, then the whole network is compromised. Thus for n users to communicate with each other securely in a network, $n(n-1)/2$ different keys are required. The number of keys thus grow as the square of the number of users who want to communicate. These keys must be distributed to the users via private and secure channels which are normally couriers. Moreover, for reliability reasons, keys must be produced and distributed not once, but constantly. They must be changed with the passage of time or when they are feared compromised.

In a large network with a large number of users, this is a mammoth if not impossible task to perform using couriers only. Only a key distribution service, using the network itself as a bearer, can make such a system feasible. This key distribution service can be provided by the network or another third party to provide automatic electronic key distribution over the network.

4.0 KEY DISTRIBUTION FUNDAMENTALS

To be able to use a cryptographic system, keys must be distributed to the communicating entities (users, processes). If bilateral key distribution is used, each principal involved in an association can reliably verify the identity of the principal at the other end. But this approach, by itself, has the problem that two principals always use the same key (call it the long term key). To extend this approach to allow a per-association key, the key must be securely distributed to each end of the association. One method of distribution is to transmit the per-association key at association initiation time, encrypted under the long term key.

Keys held for long periods of time and used exclusively for the transmission of per-association keys are referred to as master keys. One or more keys used during the course of a single association are referred to as session keys. Thus, master keys are used to authenticate principals, and to protect transmitted session keys, while session keys are used exclusively to encrypt the messages of a single association. Message key are generated for each message encrypted and are not secret. They are used to ensure that every message is encrypted with a ~~different keystream~~.

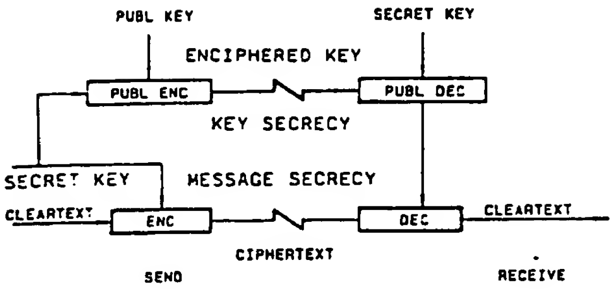


FIGURE 3: HYBRID SYSTEM

Managing such a large number of keys can be cumbersome and expensive. For example, if the master key list on a host is subverted, all users on that list must be notified. If a user loses his list of master keys, all hosts on that list must be notified. In order to reduce the proliferation of master keys significantly, the concept of trusted intermediaries such as key certification centres has been developed.

5.0 SECURE COMMUNICATION PROCEDURE FOR LARGE NETWORKS

The main objective we want to achieve with this procedure is to provide automatic key distribution over the network and also to do away with the requirement that every time a user wants to communicate with another user he must first approach a trusted third party to obtain a session key. This procedure will only need the user to contact the trusted third party once, and that is when he joins the network initially. In this way there will be no need for an on-line third party and overhead will be much reduced.

5.1 Hybrid encryption system and key certification centres.

The procedure is based on a combination of conventional systems and the public key systems to provide a so called hybrid system. The most suitable public key algorithm for this purpose is the RSA algorithm [3] developed by Rivest, Shamir and Adleman. In the hybrid system the key distribution is being done with the public key system, and the encryption of the data with a conventional system. This overcomes the problem of the slow speed of the RSA public key system and gives us the combined advantages of the speed of the the conventional systems as well as the key distribution and authentication properties of the public key system. See Figure 3 for a hybrid system and Figure 4 for a description of the basic building blocks of the user end equipment.

With only conventional encryption, for A and B to establish a secure communication link between them they must first have an exchange of secret numbers which are encryption keys. With a public key system like the RSA algorithm, A and B can establish a secure communication link between them by first exchanging non-secret public keys. In either case the exchange of numbers must be certified. That is, A must be assured that the key received are indeed from B and vice versa.

Suppose A and B are only two members of a large communications network of users where any two network users may want to establish a secure communication link at any time. An off-line network key certification center (KCC) can be established so that all users' public keys can be certified. That is, each user in the network can generate public keys and have them certified by the key certification center. After a one time certification of a public key, a user can send his certified public key to any other user who can then automatically verify its authenticity.

The KCC generates its own public and secret key and all users in the network have knowledge of the certification center's public key. The key pairs of the users can be generated by themselves or by the KCC. Assume that the KCC generate the user's key pairs. The KCC then encrypts the user's public key and identification number with his own secret key and place this together with his public key and A's secret key on a smart card. The data is encrypted on the smart card by using A's personal identification number (PIN). See Figure 5 for a description of the KCC. Also included in the certificate, is a period of validity of the certificate, which consists of two dates, the first and last on which the certificate is valid.

From this point on A will send his certified key whenever he wants to establish a secure communication link with another user in the network. Any user who receives A's certified public key can obtain the public key and identification number by decrypting it using the KCC'c public key and know that it is indeed A's public key. He will then send his certificate to A and A will then establish in the same way whether it is B's public key or not. These public keys can then be used to exchange a secret key for the actual message encryption by using a conventional encryption system.

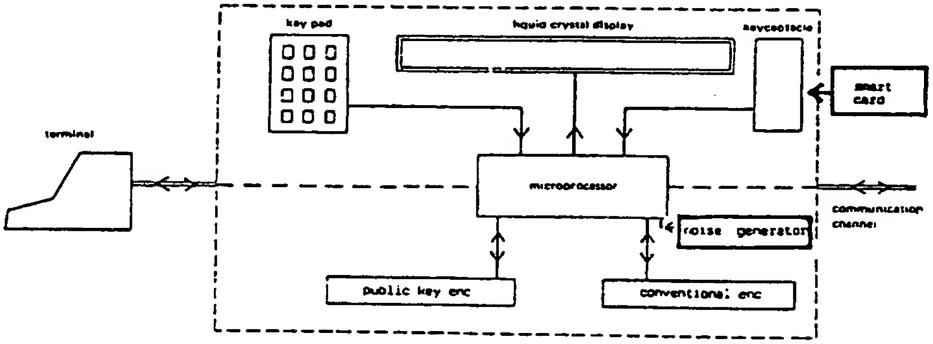


FIGURE 4: Hybrid cryptosystem end equipment

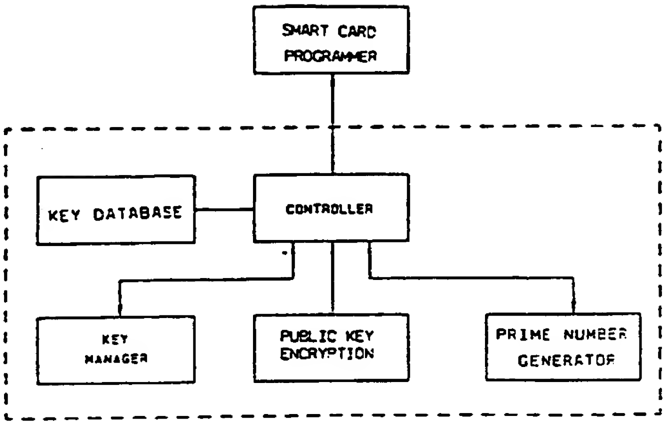


FIGURE 5: Key certification center

The procedure must also be protected against what is known as playback attacks. The only way to do this is to include authentication tokens in the certificates. The procedure is very similar to the three way strong authentication method [4] proposed by the CCITT and ISO for the Directory authentication framework. The difference is that with the CCITT proposal the user A who initiates the connection first have to obtain the public key of B, and B's certificate prior to the exchange of any information. This may involve access to the Directory of the KCC. In the proposed procedure the strong three way authentication method has been adapted to allow secure exchange of information without without having to access the KCC directory or to know B's public key. The procedure is indicated in Figure 6 and is as follow.

5.2 Details of the secure communication procedure.

Encryption of a message M with a key Ap is indicated by

Ap{ M }

The following notation is used for the description of the procedure:

A - Unique identification name of A
Ap - Public key of A As - Secret key of A
Bp - Public key of B Bs - Secret key of B
Np - Public key of certification center
Ns - Secret key of certification center
CERTa - Certificate of user A
TI - Validity period of certificate
Ra,Rb,Rc - Random numbers with sequential parts by the counters

The procedure is as follow:

1. A generates Ra, a random number, which is used to deteck replay attacks and to prevent forgery. Ra include a sequential part that is generated by Counter A and is every time checked for its value uniqueness during every session. Because Ra forms part of a token that is only signed but not encrypted, it can only be used as part of the message key for the conventional cypher and not as a part of the secret key for this cypher.

2. A then sends the following message to B:

CERTa , As{ Ra, B }

where B is the identity number of B and the latter component is the authentication token.

3. B then carries out the following actions:

a. obtains Ap from CERTa by decrypting using Np and he also checks that A's certificate has not expired.

b. verifies the signature, and thus the integrity of the signed information.

4. B generates Rb, a random number used for similar purposes as Ra. This number without the sequential part can be used to form part of the secret key because it forms part of a token that is signed and encrypted.

5. B sends the following message to A:

CERTb, Ap{ Bs{ Rb, A, Ra } }

6. A the carries out the following actions:

a. Obtains Bp from CERTb by decrypting using Np and he also checks that B's certificate has not expired.

b. deciphers the authentication token, then verify the signature, and thus the integrity of the signed information.

7. A also checks that the received Ra is identical to the Ra which was sent.

8. A then generates Rc and test it. Rc is another random number which is generated for the purpose to be combined with Rb to form the secret keys for the conventional encryption system. Once the session is over, all three the generated random numbers will be destroyed and only their sequential parts will be kept for reference.

9. A then sends the following authentication token to B:

Bp{ As{ Rb, Rc} }

10. B carries out the following actions:

a. deciphers the authentication token, then checks the signature and thus the integrity of the signed information.

b. Checks that the received Rb is identical to the Rb which was sent.

The advantages of this system is that the KCC is off-line and that the users have to approach it only once and that is when their public keys are certified when they join the network. There is thus no need to distribute lengthy directories. There is also no potential bottleneck to get a new session key from an online key distribution center each time you want to communicate. Another advantage is that the users themselves can generate their own public and secret keys or it can be done for them by the KCC. By using a hybrid system the users also have the added advantage of digital signatures and authentication.

This hybrid system can also be adapted for application in a variety of communication systems, such as point-to-point data communication, packet switching networks, electronic mail systems and EFTPOS systems.

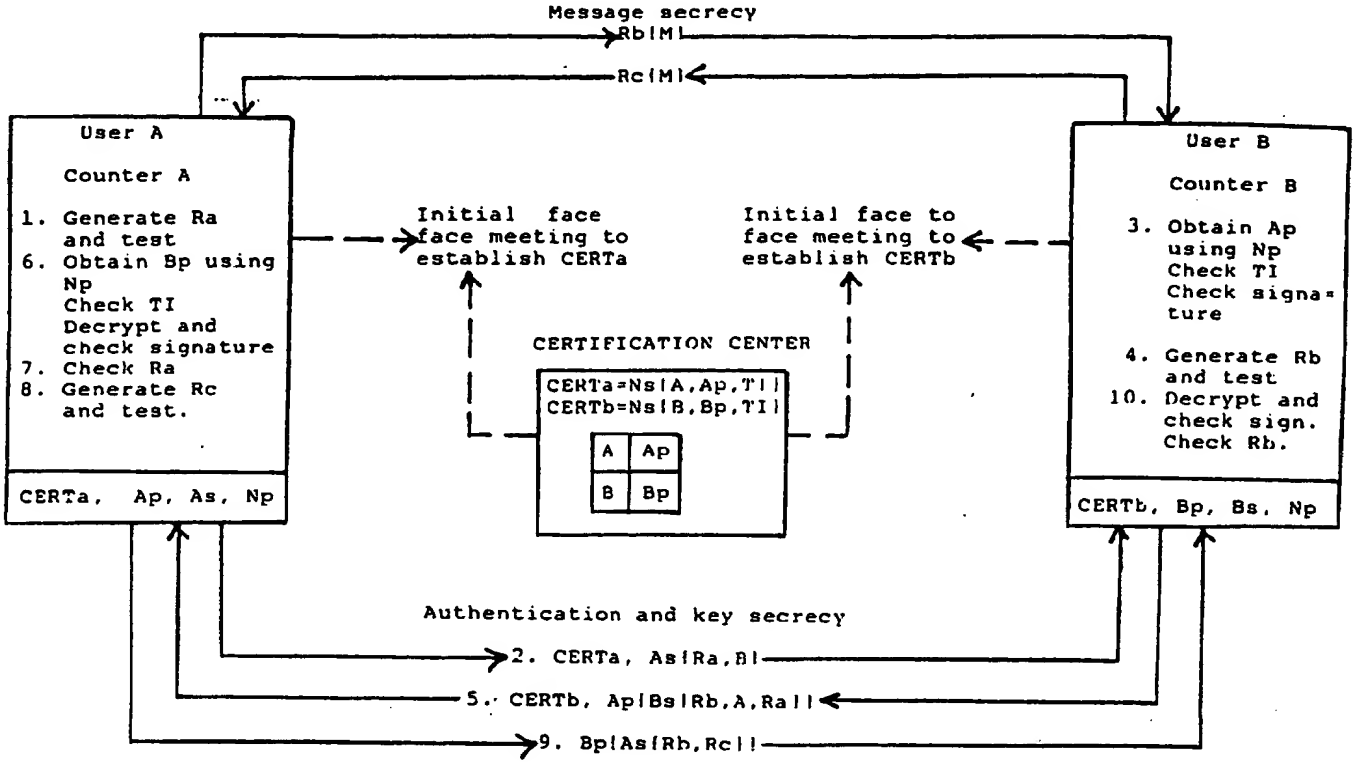


Fig. 6: Secure communication procedure based on the strong three way authentication method.

5.3 Physical security of keys

It is clear from the discussion of the KCC concept that the security of the users secret keys, is the most important aspect in the network. If these keys are compromised all communication with that specific user is compromised. Special care will then have to be taken to ensure their physical security. As they will be transported by courier, the method of protection must also be practical and highly secure.

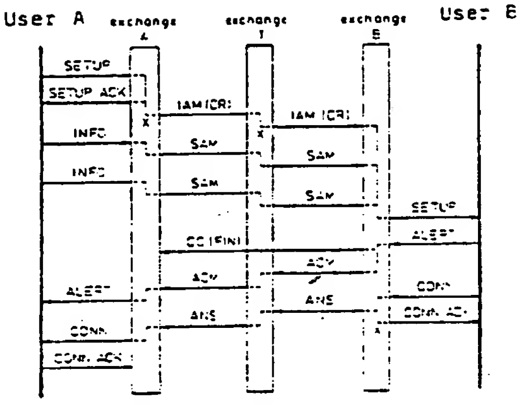
It is recommended that the best way to protect these keys is to store them encrypted on smart cards. The keys themselves are saved encrypted in the card's memory and can only be retrieved from the card if put into the correct encryption device and if the correct PIN number is given to the on-card microprocessor.

6.0 IMPLEMENTATION IN ISDN

One of the main properties of ISDN is that a signalling/data channel, independant of the information channel, is always available to the terminal equipment and can be used for key distribution and security service management. The ISDN structure and its protocols also allow for the integration of the key distribution function into the procedure for the establishment of a circuit-switched connection ([5] and [6]). We will now describe the integration into ISDN, of the procedure described in 5.0, to perform key distribution on the D-channel in association with a circuit switched connection. It is assumed that CCITT recommendations Q.910 and Q.920 are adopted for layers 1 and 2 and the layer 3 of the procedure is based on recommendation Q.930. O'Higgins [7] described a similar procedure for ISDN but which also makes use of exponential key exchange. This procedure also needs access to an online key distribution center.

Figure 7 shows a diagram of the integration in ISDN of the procedure as set out in 5.0 and the notation used. The terminal of user A initiates the call by transferring a SETUP message across the user network interface. The message contains all the normal information required from the terminal by the network to process the call as well as the certificate and authentication token of user A in the user data field as indicated. The network, after sending a SETUP ACKNOWLEDGE message to the terminal to acknowledge the SETUP message, determines whether the call can be established as requested.

Exchange A then went on to use the common channel signalling network to establish a user-information channel with exchange B as indicated. This exchange then goes on with the procedure by transferring a SETUP message across the interface of the called subscriber B. The message, in addition to the other information, includes A's certificate and authentication token in the USER DATA field. User B then establish the authenticity of A's certificate and token. If he is satisfied, he responds with an ALERT message which includes his certificate and authentication token in the USER DATA field as indicated. The originating exchange then transfers this across the calling user interface.



x: through-connection of the user-information channel

FIGURE 7: Integration into ISDN of secure procedure

A now authenticates the certificate and token of B. If he is not satisfied, the terminal sends to the network a DISCONNECT message, indicating in the message the cause of the call clearing request. The B terminal acts analogously. If for this terminal the checks are satisfactory, it sends to the network a CONNECT message and the exchange A, upon receiving it, sends a CONNECT message to the calling user interface, to indicate that the connection has been established.

The third message of the tree way authentication which consists only of A's token, is then transferred to B using the user-to-user signalling via temporary signalling connection facility. If B is satisfied after he has authenticated the token, the transmission which follows between A and B is encrypted using a key which is a combination of the random numbers Rb and Rc. B can however initiate a connection release if he is not satisfied with the authentication of A.

Even while the messages which are sent over the B-channel are encrypted, the secret key of the conventional cipher can be continually changed using the user-to-user signalling via temporary signal connection facility over the D-channel without interrupting the communications on the B-channel. ISDN D-channel signalling also makes calling party identification available from the network and this is one more level of security that can be applied.

7.0 CONCLUSION

Privacy and authentication are the two most important security requirements in communication networks and encryption is the most appropriate and practical mechanism to provide communication security.

A secure communication procedure based on a hybrid encryption system and the strong three way authentication method of the CCITT and ISO is proposed as an effective solution of the key distribuion problem. The most important advantage of this procedure is that the user need only to approach a trusted third party once, and that is when he join the network.

In a hybrid system a public key algorithm is used to distribute secret keys over the network which are then used as the keys for a conventional system to encrypt the data messages. The KCC must be based on a hybrid system which make use of the RSA algorithm. It is also recommended that the encryption keys be kept on smart cards to ensure that they do not get compromised.

It is shown that ISDN offers many advantages compared to the current switched telephone network. The ISDN structure and its protocols allow for the integration of the key distribution and authentication function in the procedure for the establishment of a circuit switched connection. Signalling on the D-channel can be used to monitor and update keying information on the terminal, even while B-channels are active and without deactivating the channel. The packet data service on the D-channel also provides an efficient means of communication to a centralized key management facility if only conventional ciphers are used. Another advantage due to ISDN signalling is that calling party identification is available, which is another security element that can be used to authenticate users and connections.

There is increasing concern for information security in civil communication systems. These security services are beyond what can be delivered using only the current network, but they are within the capabilities of ISDN.

REFERENCES

[1] Voydock, V.L. and Kent, S.T., "Security in high-level network protocols", IEEE Communications magazine, July 1985, Vol. 23, No. 7, pp. 12-24.

[2] American National Standards Institute, "American National Standard, X9.17, Financial Institution Key Management (Wholesale)", 1984. Developed by ANSI X9.17 financial services.

[3] Rivest, R.L., Shamir, A. and Adleman, L., "A method for obtaining digital signatures and public key cryptography", Communications of the ACM, Vol. 21, pp. 120-126, 1978.

[4] CCITT, "CCITT Draft recommendation X.509 (Version 6) The Directory Authentication Framework", CCITT Question 35/SG VII Meeting, Geneva, June, 1987.

[5] Improta, S., "Privacy and authentication in ISDN: The key distribution problem", Note Recens and Not (Italy), Vol. 33, no 1-2, Jan-June 1984, pp. 27-33.

[6] Prestun, K., "Security measures in communication networks", Electrical communication (GB), Vol. 60, No. 1, 1986, pp. 63-79.

[7] O'Higgins, B., Diffie, W., Strawczynski, L. and De Hoog, R., "Encryption and ISDN - A natural fit", IEEE International Switching Symposium 1987, March 15-20, 1987, Phoenix, Arizona, pp. A11.4.1-7.

[8] Meyer, C.H. and Maytas, S.M., "Cryptography: A new dimension in data security", John Wiley and Sons, 1982.